

LA SIGNATURE ELECTRONIQUE DANS LES MARCHES PUBLICS - MODE D'EMPLOI

Les règles d'usage de la signature électronique dans les marchés publics sont fixées dans l'arrêté du 15 juin 2012 relatif à la signature électronique dans les marchés publics, qui s'est substitué à l'arrêté du 28 août 2006.

Mode d'emploi pour accompagner la généralisation de la dématérialisation, l'arrêté précise et uniformise les conditions d'utilisation de la signature électronique, quel que soit le signataire (personne publique ou opérateur économique) ou le document à signer. Rappel de l'essentiel :

1. A qui s'adresse ce texte (article 1er de l'arrêté) ?

A tous les utilisateurs potentiels des marchés publics : autorités administratives et opérateurs économiques.

La personne qui signe électroniquement est celle qui aurait signé le même document de manière manuscrite : c'est la personne habilitée à engager l'organisme qu'elle représente. La signature électronique se substitue directement à la signature manuelle : elle permet d'identifier le signataire.

2. Quels sont les documents concernés (article 1er de l'arrêté) ?

Les documents transmis électroniquement sont signés électroniquement dès lors qu'une signature est requise. La signature peut être prévue par le code des marchés publics (cas de l'acte d'engagement, pour les marchés formalisés), par les documents de la consultation, ou dans le document lui-même (certains formulaires DC, par exemple).

L'arrêté n'élargit ni ne restreint le champ des documents à transmettre revêtus d'une signature : les documents à signer électroniquement sont ceux qui auraient été signés de manière manuscrite. C'est le mode de transmission (papier ou électronique) qui détermine la manière de signer (signature manuscrite ou électronique). En revanche, un document pour lequel aucune signature n'est requise sera transmis électroniquement sans signature électronique.

Il est recommandé aux acheteurs de mentionner précisément, dans les documents de la consultation, les documents qu'ils veulent voir transmis signés, en rappelant qu'en cas de transmission électronique, la signature électronique est requise sur le document lui-même (un fichier zip signé ne vaut pas signature de chaque document qu'il contient, ou encore une signature manuscrite scannée n'a pas valeur d'original signé).

Rappel : ne pas exiger la signature des documents qui sont des annexes à l'acte d'engagement ; il suffit de les lister dans l'acte d'engagement, et les identifier précisément (numéro de version, nombre de pages).

3. Est-il possible de limiter les certificats de signature électronique acceptés (article 2-I de l'arrêté) ? De limiter les formats de signature (article 3 de l'arrêté) ? Peut-on imposer l'utilisation de l'outil de signature proposé sur le profil d'acheteur ?

Le principe posé est que l'utilisation de tout produit est possible, à partir du moment où il présente des garanties de sécurité suffisantes et où le destinataire du document signé est en mesure de procéder à la vérification de la signature.

L'arrêté élargit les catégories de certificats utilisables, qui sont (cf. infra : *lien utiles*) :

- les certificats référencés en France, ou figurant sur la liste de confiance d'un Etat-membre de l'Union européenne ;

- les certificats qui ne figurent pas sur une liste de confiance, qui doivent présenter un niveau de sécurité suffisant (la référence pour les administrations étant le référentiel général de sécurité, l'arrêté précise que ces certificats répondent à une norme équivalente à celle du RGS). Il s'agit de certificats conformes au RGS mais non référencés sur une liste, ou de certificats qui présentent un niveau de sécurité équivalent.

Le signataire s'assure que le certificat qu'il utilise présente au moins un niveau de sécurité équivalent à celui préconisé sur le profil d'acheteur, et donne tous les éléments nécessaires à la vérification de sa signature par le profil d'acheteur.

Par ailleurs, une décision de la Commission européenne de février 2011 impose d'accepter les formats de signature XAdES, PAdES et CAdES cités à l'article 3 de l'arrêté. Les trois formats doivent être acceptés par le profil d'acheteur, qui peut néanmoins prévoir d'accepter des formats supplémentaires. Cette possibilité est alors mentionnée dans les documents de la consultation ou la lettre de consultation.

Tout outil de signature conforme à ce qui précède est utilisable. L'acheteur ne peut pas imposer l'emploi de l'outil de la plateforme. Néanmoins, lorsque l'opérateur économique utilise un autre outil de signature, il en permet la vérification en transmettant en parallèle les éléments nécessaires (mode d'emploi) pour procéder à la vérification de la validité de la signature et de l'intégrité du document, et ce, gratuitement.

4. Comment vérifier la conformité du certificat de signature à un niveau de sécurité équivalent au RGS (article 2-II de l'arrêté) ?

L'ordonnance n° 2005-1516 du 8 décembre 2005 prévoit que l'autorité administrative détermine pour chaque système d'information, et après étude, le niveau de sécurité requis parmi les niveaux prévus par le RGS (niveau *, ** ou ***). Les échanges intervenant via le système d'information respectent par la suite les règles correspondantes. Par exemple, si le profil d'acheteur requiert un niveau de sécurité ** du RGS, tous les produits utilisés sur le profil d'acheteur, dont le certificat de signature électronique, devront correspondre au moins aux préconisations du niveau ** du RGS. Cela signifie que la plateforme devra reconnaître et accepter les produits de niveau ** et ***, mais pas ceux de niveau *.

L'arrêté prévoit plusieurs cas selon le certificat de signature utilisé :

- ***le certificat de signature est référencé ou émane de la liste de confiance française ou d'une liste de confiance d'un autre Etat-membre***

  Dans ce cas, la conformité du produit au RGS est présumée, et les seules vérifications à opérer sont celles du niveau de sécurité (*, ** ou ***) et bien sûr, de la validité de la signature elle-même. Le signataire n'a pas à fournir d'autres éléments que ceux permettant la vérification de la validité de la signature.

- ***le certificat de signature électronique n'est pas référencé ni ne figure sur une liste de confiance*** : il peut s'agir de produits émanant de prestataires de pays-tiers, mais aussi de prestataires européens ou français, qui n'ont pas fait l'objet d'un référencement, souvent pour des raisons de coût. Ce sont ces certificats qu'il faut vérifier avant de les accepter. L'arrêté prévoit que le signataire transmet les éléments nécessaires à cette vérification, en plus des éléments nécessaires à la vérification de la validité de la signature elle-même. Cela peut être l'adresse du site internet de référencement dans le pays tiers, une preuve de la qualification du prestataire ou du produit, l'adresse de l'autorité de certification qui a délivré le certificat de signature, qui mentionne la politique de certification…

5. L'acheteur est-il tenu d'effectuer lui-même ces vérifications techniques?

Non. La vérification des certificats de signature électronique et de la validité de la signature elle-même font partie actuellement des fonctionnalités d'un profil d'acheteur, sans que l'acheteur ait dû se doter des compétences techniques pour les examiner. L'automatisation et la traçabilité des vérifications et contrôles doivent continuer à être privilégiées.

En revanche, la vérification de l'identité du signataire, et de sa capacité à engager l'entreprise, reste, comme pour les marchés non dématérialisés, effectuée par l'acheteur.



Si une décision doit être prise sur le rejet d'une candidature ou d'une offre du fait de la non-conformité de la signature électronique, cette décision revient, toujours, à l'acheteur, qui reste responsable de tout le processus d'achat. A ce titre, l'arrêté ne modifie pas les responsabilités de l'acheteur.

*

*   *

Il est recommandé de préciser dans les documents de la consultation :

- un rappel du niveau de sécurité requis sur le profil d'acheteur (niveau *, ** ou *** conforme au RGS) ;
- les documents pour lesquels une signature manuscrite ou le cas échéant électronique est requise ;
- les formats de signature autorisés (et toujours au moins, les trois formats cités à l'article 3 de l'arrêté) ;
- le rappel à titre pédagogique de certaines règles courantes : un zip signé ne vaut pas signature de chaque document du zip, une signature manuscrite scannée n'a pas d'autre valeur que celle d'une copie et ne peut pas remplacer la signature électronique qui confère valeur d'original au document signé.

Liens utiles :

- Documents de référence de l'administration électronique : RGS et référencement
- Liste des organismes habilités au référencement (RGS)
- Liste des offres référencées (RGS)
- Liste de confiance française
- Liste de confiance européenne